



This Notice applies to Lightbox and its subsidiaries

## General Data Protection Policy (including Staff Records)

### Scope of the Policy

At Lightbox Media we hold information protected by the General Data Protection Regulations (GDPR) and the Data Protection Bill 2018, including personal data about our employees and staff, clients, suppliers, customers and other individuals, for a variety of business purposes.

Reference to **Processing** in this policy is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

**Everyone** working for us has a legal obligation to ensure that we comply with the requirements of the GDPR and follow the safeguards we have implemented in order to best protect all the Personal Data we hold.

This policy sets out how the Company will seek to protect personal data and individuals' rights and obligations in relation to their personal data. This policy should be read in addition to our Policy relating to staff use of the internet and e-mail (Computer and IT Policy).

The person responsible for this policy in the Company is Vanessa Tovell, Chief Operating Officer.

**This Policy should be regarded as a living document that may be amended by us at any time, to ensure our ongoing compliance with The General Data Protection Regulations (effective 25<sup>th</sup> May 2018) and the UK's Data Protection Act 2018.**

### The reasons we process personal data is to:

- Undertake research for our business
- Recruit, support, manage and pay our staff
- Manage our on-air talent and contributors
- Maintain our Accounts and Records
- Market and Promote our Goods and Services
- Respond to Enquiries and Complaints
- Maintain the security and safety of our property, premises and IT systems
- Ensure a safe working environment.

### Definitions

**Personal Data** is data we gather which relates to a living individual who can be identified from that data, or from that data in conjunction with other readily available information, e.g. their name, address, images, telephone numbers, personal email addresses, date of birth, bank and payroll details, next of kin, passport particulars etc. It can also include data such as IP addresses and data automatically collected when using computers and the internet, as well as educational background (certificates, diplomas, education, skills, CV), skills, marital status, nationality, job title, contact details, references, attendance records, performance records and so on.

This data may be collected from the individual themselves or provided by other parties, and may be in paper or electronic format.

**Special Category Data** is data that relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), physical or mental health matters, sexual orientation/life, genetic and biometric data.

**Criminal Records data** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

### **Our Data Protection Principles**

The GDPR protects individuals' rights concerning information about them that is held on computer. Anyone processing personal data must comply with the eight principles of good practice, which are that data must be:

- fairly and lawfully processed (in accordance with individuals' rights)
- adequate, relevant and not excessive (limited to what is necessary for the purpose of processing)
- collected only for specified, explicit and legitimate purposes (including for business purposes to comply with legal, regulatory, corporate governance obligations and good practice)
- accurate and kept up to date (we take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay; and Individuals can ask that we correct their inaccurate personal data).
- not kept longer than necessary for its original purpose
- processed in accordance with the data subject's rights and its specified purposes
- secure (i.e. appropriate measures have been taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or, or damage to, personal data)
- not transferred to countries or territories outside the EEA unless that area ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this, or would otherwise reasonably expect this.

### **Conditions for Processing Personal data**

The processing of personal data will only be fair and lawful when the purpose of the processing meets a legal basis (see below) and when the processing is transparent. This means we will provide people with an explanation of how and why we process their personal data, in a Privacy notice.

Processing of personal data is only lawful if at least one of these legal conditions is met:

- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another

person

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.
- If none of these legal conditions apply, the processing will only be lawful if the data subject has given their **clear, explicit, consent**.

Where we are required to get consent from the data subject, we will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting consent for and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

Consent can however be withdrawn by the individual at any time and if withdrawn, the processing must stop. Data subjects will be informed of their right to withdraw consent and it must be made as easy to withdraw consent as it is to give consent.

### **Privacy Notices - transparency of data protection**

Being transparent and providing accessible information to individuals about how we will use their personal data is important for the Company. Privacy notices for job applicants, staff, contributors, can be found at [www.lightboxent.com](http://www.lightboxent.com) or in the 'Policies & Procedures' section of the Staff Handbook.

The Privacy Notice:

- Must be given at the point their data is collected from them (or collected about them from other sources) and gives our identity/contact details;
- Sets out the purposes for which we hold an individuals' personal data;
- Explains the legal basis for processing; if the data is to be sent outside the European Union, how long the data will be stored for;
- Highlights that sometimes the Company may be required to give information to third parties;
- Explains the individuals data subjects' rights.

This information will be provided to the individual in writing and no later than within 1 month after we receive the individuals data, unless a legal exemption under the GDPR applies.

### **Special Categories of Data and Criminal Records Data**

In the limited cases where the Company processes special categories of data, this requires extra care and is usually only lawful when, in addition to one of the conditions above, one of the extra conditions, as listed in Article 9 of the GDPR, is met. These conditions include where:

- the processing is necessary for carrying out our obligations under employment and social security and social protection law;
- the processing is necessary for safeguarding the vital interests (in emergency, life or death situations) of an individual and the data subject is incapable of giving consent;

- the processing is carried out in the course of our legitimate activities and only relates to our members or persons we are in regular contact with in connection with our purposes;
- the processing is necessary for pursuing legal claims.
- If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their explicit consent.

We will not hold information relation to criminal proceedings or offences or allegations of offences unless there is a clear lawful basis to process this data such as where it fulfills one of the substantial public interest conditions in relation to the safeguarding of children and of individuals at risk, or because it is necessary for us to carry out our statutory or regulatory obligations and exercise specific rights in relation to employment, or it meets one of the additional conditions relating to criminal convictions set out in either Part 1 or 3 of Schedule 1 of the Data Protection Regulations 2018.

### **Data Security**

We keep personal data secure against loss, accidental destruction, misuse or disclosure and we have internal policies and controls in place to protect data.

The Company will ensure that data is not accessed except by any staff other than those who need to in the proper performance of their job.

Where other organisations process personal data as a service on our behalf, the Chief Operating Officer will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

### **Privacy by design and default**

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Chief Operating Officer will be responsible for ensuring that all new data security processes and IT projects commence with a privacy plan.

### **Impact analysis exercises**

Where data is processed that could result in a high risk to an individuals rights and freedoms, the Company will carry out a data protection impact assessment (DPIA) to determine the necessity and proportionality of the processing. For example, this would apply if we were to consider using CCTV cameras within the workplace, or we need to process data relating to vulnerable people, trawl data from public profiles, introduce new technology, and transfer data regularly outside the EU.

Any decision not to conduct a DPIA will be recorded. DPIAs will be conducted in accordance with the ICO's Code of Practice 'Conducting privacy impact assessments'.

### **Data retention periods**

We retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained. The length of retention will be determined in a manner consistent with published legal and regulatory data retention guidelines.

Data retention periods are explained in our relevant Privacy Notices.

### **Data deletion**

The Chief Operating Officer is responsible for ensuring that records that are no longer required are reviewed as soon as possible so that, where appropriate, records are destroyed. Some records may instead be selected for permanent preservation, digitised to an electronic format or retained by the organisation for litigation purposes.

### **Transferring data internationally**

There are restrictions on international transfers of personal data. Personal data must generally not be transferred outside of the European Economic Area unless the receiving country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data, unless the data subject has given their consent and:

- (a) The transfer is necessary for the performance of a contract between the data subject and the data controller, or
- (b) The transfer is necessary for certain contracts with third parties, or
- (c) The transfer is necessary to protect the vital interests of the data subject.

Lightbox has a US office with which data is shared on a regular basis in order to carry out our business activities. The US is considered by the ICO to have an adequate level of protection for the rights and freedoms of data protection subjects.

Otherwise adequate safeguards must be put in place and other conditions must be met. **You should refer to the Chief Operating Officer if you are unsure whether this need applies.**

### **Storing data securely – ALL STAFF MUST FOLLOW THESE PRINCIPLES:**

- Ensure personal data is not left lying around on your desk. Files containing special category/sensitive data and financial data should be locked/password protected
- Avoid printing and when it is necessary, printed paper should be shredded when it is no longer needed
- Regularly update your computer password and password protect any personal devices
- Emails containing others personal data should only be sent from company e-mail accounts
- Restrict access to information whether on computer or hard copies to only those who are authorised or need to have access to it. Where documents contain personal data (and relatively few documents don't) ensure that they are electronically stored either in a secure part of the server/Box with the appropriate access limitations or within an encrypted/password protected folder. Ensure others in receipt of the information are aware of the need to keep the information protected and know when it should be deleted (or returned to you)
- Ensure antivirus and malware software are up to date as well as operating systems on all devices. Be careful when opening unrecognised emails and attachments or visiting new websites to prevent viruses
- Computers, laptops, memory sticks etc., taken off the premises must have appropriate protection

- Any sensitive/special category data, or children's/vulnerable adults, contributors or financial data must be encrypted if taken off the premises
- Staff must report a loss of any device immediately to their manager/the person responsible for Data Protection in the Company
- At the end of your employment with the Company you must return all confidential and/or personal data and Company equipment, and delete all the information relating to the Company from any personal computer, mobile or other equipment you were using/own

### **Individual Responsibilities in your job**

Staff may have access to the personal data of other individuals (staff, crew and contributors) in the course of their employment. Where this is the case, the Company relies on individuals to help it meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- To comply with this Policy and follow the 'storing data security' points above;
- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction).

If you think you have accidentally breached this policy it is important that you contact Vanessa Tovell on +44 20 3750 0922 immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate and/or reckless breaches of this policy (including for personal benefit), such as accessing employee, contributor or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

In particular, please remember that if you receive a request from outside the Company for any information about your colleagues, contributors, our customers or suppliers, you should pass this request on to the individual themselves with details of the person who enquired so that the individual can confer with them directly, or alternatively check with the Chief Operating Officer whether it is possible to release the information before doing so.

If you are a Manager you should ensure you follow the rules set out in this Policy and that the staff you are responsible for, do so as well.

### **Training**

All staff will be made aware of their obligations and responsibilities in line with the new General Data Protection Regulations that become law on 25<sup>th</sup> May 2018.

## **Data Breaches**

In the event you become aware of a breach of security or an unauthorised disclosure or loss/theft of documents/data, you should alert Vanessa Tovell immediately.

Data breaches that are likely to result in a risk to any person need to be reported to The Information Commissioners Office (ICO) within 72 hours of discovering the breach. This will be done by Vanessa Tovell. Any data breach should be immediately discussed with Vanessa Tovell prior to any further action being taken.

In situations where a personal data breach causes a high risk to any person, we will (as well as reporting the breach to the ICO), inform data subjects whose information is affected, without undue delay. This can include situations where, for example, bank account details are lost, or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.

## **Individuals Rights**

Individuals have a number of rights in relation to their personal data:

### **Subject access requests**

Under GDPR, individuals are entitled, subject to certain exceptions, to request access to information held about them. No charges should be made to the data subject to provide this information. Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed by the Company within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system.

If you receive a request from a data subject that relates or could relate to their data protection rights, please forward this to Vanessa Tovell, Chief Operating Officer.

If you would like to make a subject access request about your own records, you should refer that request to Vanessa Tovell, Chief Operating Officer. In some cases, the Company may need to ask you for proof of ID before the request can be processed.

If a subject access request is manifestly unfounded or excessive the Company is not obliged to comply with it.

### **Other rights**

Individuals have a number of other rights in relation to their personal data. They can require the Company to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and

- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

To ask the Company to take any of these steps, the individual should send the request to [info@lightboxent.com](mailto:info@lightboxent.com).

### **Sharing information with other organisations**

We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of their data being shared (in a Privacy Notice), unless legal exemptions apply to informing data subjects about the sharing. Only authorised and properly instructed staff are allowed to share personal data.

### **Staff/HR Records**

At Lightbox Media we also collect personal data on job applicants, employees, workers, contractors/freelancers, agency workers, interns and of former employees.

As your employer, we need to keep information on record relating to your employment and it is necessary to keep and process personal data and it may be necessary to process special category data.

The purposes for which this data may be processed are:

- To facilitate Recruitment
- Payroll, to enable your salary to be paid accurately, and to fulfil our obligations to the HMRC
- Absence management and Accident Reporting
- Equal Opportunities monitoring (if, in the future we may choose to do this)
- Performance Management
- Pension and Benefit purposes
- To make statutory payments to you that you are due (e.g. Maternity Pay and Statutory Sick Pay)
- To contact your next of kin in an emergency
- To ensure we meet our obligations to you regarding holidays and rest breaks
- To ensure we provide a safe working environment
- To provide information at the request of legitimate 3<sup>rd</sup> parties
- To confirm your right to work in the UK (a copy of the documents that you supplied on appointment showing your Right to Work in the UK are kept on your personnel file).

Procedures are in place to protect the confidentiality of your data so that access is restricted to those with a relevant need to do so. Data will be held in an individual personnel file (in hard copy or electronic format, or both) and on HR systems. The purpose for which the Company holds staff records are contained in its Privacy Notices to staff, as are the periods for which the HR related personal data is retained.

The Company will keep a record of its processing activities in respect of staff data in accordance with GDPR requirements. Specifically:



- Where the Company is required to undertake criminal records checks of its staff, we will not hold information relation to criminal proceedings or offences or allegations of offences unless there is a clear lawful basis to process this data such as where it fulfils one of the substantial public interest conditions in relation to the safeguarding of children and of individuals at risk, or because it is necessary for it to carry out its statutory and regulatory obligations and exercise specific rights in relation to employment, or it meets one of the additional conditions relating to criminal convictions set out in either Part 1 or 3 of Schedule 1 of the Data Protection Regulations 2018.
- Where the Company processes sickness and health records the Company does so to ensure a safe working environment for all workers, to maintain records of statutory sick pay, to maintain accident reports and to ensure disabled staff are not discriminated against and possible reasonable adjustments to their workplace are identified. Where the Company requires an employee or job applicant to undertake a medical questionnaire, examination or report it does so to gather information on their ability to do the job they are applying for (job applicants) and, for employees, to gather information on their fitness to work when the employee has had a long-term absence, or for example as part of a contractual sick pay scheme. Job Applicants and Employees will be asked to give their explicit consent for the company to gather medical information on them and for the medical report to be released to the Company. The individual employee may withdraw their consent to this at any stage.

**For all staff** - Please remember to notify your Manager should any of your personal details change, including home address, next of kin, bank details, and so on. (Please refer to the 'Personnel Records' section of the Handbook).

Information given in references about staff to third parties references must comply with GDPR requirements.

**From/after 25<sup>th</sup> May 2018, existing Data Protection clauses in staff contracts/agreements with the Company are unlikely to be legally compliant with the new General Data Protection Regulations (GDPR). Therefore all existing staff will receive a Privacy Notice that will override any invalid data protection clauses in their existing contract of employment/agreement with the Company, and will be asked to sign and return one copy of this Privacy Notice to the Company, to signify their acceptance of these changes. All new staff after this date will also receive this Privacy Notice.**

### **Sharing HR personal data**

It is often necessary to share Staff personal data with third party organisations (**Data Processors**). It is our responsibility to ensure that the data we share is compliant with the conditions of processing and is shared in a secure manner.

Before appointing a contractor who will process personal data on our behalf (a data processor) we will carry out due diligence checks. The checks are to make sure the processor will use appropriate technical and organisational measures to ensure the processing will comply with data protection law, including keeping the data secure, and upholding the rights of data subjects. We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

Third parties who we share your data with may include:

- HR providers
- Payroll providers
- Recruitment agencies
- IT Consultants
- Banks
- Pension and benefit providers
- Local Authorities and Government Departments, including the HMRC
- External accountants
- Occupational health providers
- Insurance providers
- Broadcasters
- Financiers
- Marketing
- PR

HR related personal data may also be **transferred to countries outside of the EEA** the basis that the transfer is necessary for the Company's legitimate interests to operate our business, which we believe do not supersede your rights as a data subject. We will only transfer data outside the EU where it is permitted by one of the conditions for non-EU transfers in the GDPR. We will therefore assess all the circumstances of the transfer before it happens and provide suitable safeguards to protect your personal data.

### **Consequences of failing to comply with our Data Protection Policies**

The Company takes the compliance with this policy very seriously as failure to comply puts the staff and the Company at risk. Everyone working at the Company must observe this policy.

The importance of this policy means that your failure to comply with any of its requirements may lead to disciplinary action under our Disciplinary Procedures which may result in dismissal.

If you have any questions or concerns about anything in this Policy, do not hesitate to contact Vanessa Tovell, Chief Operating Officer.

**On 25<sup>th</sup> May 2018 The General Data Protection Regulations become law in the UK and this policy should be seen as a living document which may be reviewed further and amended in the future to ensure it is compliant with the GDPR and the UK's Data Protection Act 2018.**

### **Data Protection Policy for Productions**

It's important to protect living individuals' data. Under the GDPR there can be criminal and civil sanctions for the production company when there is an unauthorised disclosure of personal and sensitive/special category data, as well as reputational damage for Lightbox.

At our Company the Chief Operating Officer is responsible for complying with the GDPR. You should contact her when you are unsure of your obligations under the GDPR when collecting, using, processing, accessing and destroying personal data.

This policy applies to **all staff employed by the Company**, including PAYE employees, freelancers, crews and Contractors.

### **Collecting and accessing personal data**

You will have access to or routinely acquire personal data and sensitive/special category personal data in many forms. This information may be from past, current and future employees, contributors, suppliers and contractors.

This information may be in the form of letters, e-mails, social media pages, correspondence, call logs, programme treatments, running orders, CV's, CCTV footage, contributor agreements/consent or release forms, contributor application/checklist forms, call sheets, P-as-Cs, disclosure & barring service checks, medical records, invoices, purchase orders, rushes with captions, bank statements, list of employees, and employee references. The information can be in hard copy form e.g. original or copy paper document, photographs and film; or in electronic form e.g. PC, laptop, mobile phone, blackberry or memory stick.

### **What should you collect?**

You should only collect data that you actually need or are likely to need. For example it may be reasonable to collect the name and contact details of contributors but it is very unlikely you would need information regarding their sexual history or their medical details (any special category/sensitive data) unless it was relevant to the programme.

When checking contributor's personal information, make the checks relevant to the type of programme you are making. These may include proof of identify and address, personal/professional references, DBS checks, health information. If you use Google search, Facebook/twitter/other social media, dating websites, bankruptcy searches to conduct checks you will need to justify why this is necessary.

### **What do you have to tell the person who is giving you the information?**

You should tell the person why you are collecting the information and what you are using it for and how it will be shared, and remind them that they are protected by the GDPR. You should tell them who you are (Lightbox), the nature of the programme and the nature of their contribution and how it will be used in the programme. You should inform them of the likelihood of repeats/future TX.

You can do this by giving them a written privacy notice or referring them to the information on our website. If you are collecting sensitive/special category data you must ensure the person receives the privacy notice.

### **How can you use the information?**

You can only use personal data for the purposes for which it was collected or given to you. For example, it may be that the personal data was only provided by a contributor for the purposes of a particular Programme and not for any other use. However if you obtain explicit consent from the person to contact them in the future to be involved in other programmes, or to receive marketing information or to contact them for other opportunities, then you are permitted to do so. This can be expressly agreed when the contributor signs the relevant consent form or at the point they provide their information e.g. in an application form.

## **Anonymisation**

Effective anonymisation can be used to publish data which would otherwise be personal data. The ICO defines Anonymisation as the process of rendering data into a form which does not identify individuals and where identification is not likely to take place through its combination with other data. A risk assessment should be carried out before such anonymised data is published.

Anonymisation might be used where audience members wish to share their stories or experiences, but the data provided is sensitive. For example, if individuals wanted to contribute to a story about their experiences with the NHS, those contributions might need to be aggregated or anonymised in order to provide support for a story without linking it to a specific individual.

## **Keeping Contributors Details Safe**

Contributor checklists must be completed and safely stored for each production, during and after filming. This information should only be shared with staff who require the information to do their job. Please familiarise yourself with the Contributors Privacy Notice that all potential and actual Contributors to our programmes will be sent.

Data of unsuccessful applicants will be retained for as short a period of time as possible, although we will often have an ongoing legitimate interest in retaining their data.

Data of Contributors who have appeared on a show may be kept indefinitely as we have an ongoing legitimate interest in retaining the data.

Written release notes must be obtained before or after filming. Where this is not possible a verbal release to camera must be obtained and date/time stamped.

Parental consent must be obtained for all under 18's (from the parent/guardian that has sole custody, or both parents/guardians if they have joint custody).

## **Other**

If you receive a request from the police for information you should advise the Chief Operating Officer immediately, who will, where appropriate seek prompt advice from your commissioning broadcaster. Where the request relates to programme material including rushes, the COO will consult with your commissioning broadcaster if appropriate before making any disclosure as there may be legitimate legal and editorial grounds for resisting disclosure.

On close down of a production Line Producers/Production Managers will review what personal data records can be legitimately retained or destroyed. There may be reasons outside of the production that might require the production company to legitimately retain information for legal or business purposes, for example there may have been an accident or ongoing litigation where documents must be preserved by law. You should ensure that you have the necessary internal permission when destroying information.

Ensure you have returned and/or destroyed documents, memory sticks, drives etc to Lighthbox.